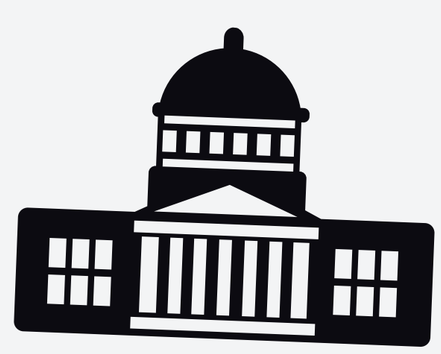
Tax Phishing Season

TAX SEASON CAN BE STRESSFUL. SPEAR PHISHERS, HOWEVER, LOOK FORWARD TO IT.

Spear phishers design fake emails and websites to spoof trusted agencies and organizations. After gaining the target's trust, attackers trick them into sharing confidential information, clicking links, downloading attachments, or wiring money.

WHO DO SCAMMERS IMPERSONATE?



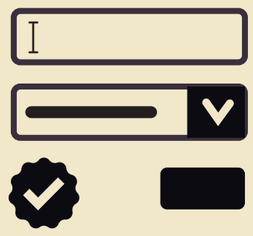
GOVERMENT AGENCIES

TAX SOFTWARE COMPANIES

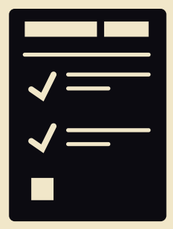
COLLEAGUES

EXAMPLES OF POPULAR TAX PHISHING SCAMS

REFUNDS



VERIFYING INFORMATION



FILING STATUS

TAX FORMS

KEEP THESE TIPS IN MIND TO AVOID FALLING FOR A TAX PHISHING SCAM

MAKE SURE THE URL IS CORRECT

Don't be misled by sites claiming to be a government agency or tax software company but have a slightly different URL.

BOOKMARK TAX SOFTWARE WEBSITES

Only navigate to trusted sites by using bookmarks.

ALWAYS VERIFY

It's easy to fake a from or reply-to address, so don't assume an email is legitimate by looking at the header. Call the sender to confirm the request is legitimate.

DON'T BOTHER OPENING IT

If the email mentions any tax forms, it's likely a scam. Most tax-related government agencies do not initiate contact by email, text message, or social media.

PHISHME